Attorney Docket No. 9407-3 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Jeffrey S. Bardsley et al.
Application No.: 10/624,344
Filed: July 22, 2003
For: SYSTEMS, METHODS AND DATA STRUCTURES FOR GENERATING COMPUTER-ACTIONABLE COMPUTER SECURITY THREAT MANAGEMENT INFORMATION

Confirmation No.: 7591
Group Art Unit: 2132
Examiner: F. Homayounmehr

February 2, 2007

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

Sir:

This *Appeal Brief* is filed pursuant to the *Notice of Appeal to the Board of Patent Appeals and Interferences* filed concurrently herewith in response to the *Final Office Action* ("Final Action") mailed December 21, 2006.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. § 1.136(a). Any additional fees believed to be due may be charged to Deposit Account No. 09-0457.

Real Party In Interest

The real party in interest is assignee International Business Machines Corporation of Armonk, New York.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Claims 1-23 remain pending, each of which is finally rejected. Appellants appeal the final rejection of Claims 1-23. The attached Claims Appendix presents the pending claims as finally rejected in the *Final Action* mailed December 21, 2006.

Status of Amendments

The attached Claims Appendix presents the claims as they currently stand. An *Amendment* was filed in this case on October 11, 2006 in which independent Claims 1, 9 and 18 were amended. This October 11, 2006 *Amendment* was entered. No Response after Final was filed.

Summary of Claimed Subject Matter

I. Claim 1

Independent Claim 1 is directed to a method of generating computer security threat management information. As shown in **Fig. 3** of the present application, the method of Claim 1 includes three operations, **310**, **320** and **330** which are generally described at page 9, line 25 through page 10, line 3 of the present application. In the first operation **310**, notification of a computer security threat is received. In operation **320**, a computer-actionable Threat Management Vector (TMV) such as, for example, the TMV **400** illustrated in **Fig. 4** of the present application is generated from the notification that was received in operation **310**. This TMV (e.g., TMV **400**) is suitable for use by an automated threat management system such as automated threat management systems that are located at the Target Systems **540** illustrated in **Fig. 5** of the present application. In the method of Claim 1, the TMV (e.g., TMV **400**) includes a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat (e.g., field **401** in **Fig. 4** of the present application), a second computer-readable field that provides identification of a release level for the system type (e.g., field **402** in **Fig. 4** of the present application) and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (e.g., field **403** in **Fig. 4** of the present application). As illustrated in operation **330** of **Fig. 3**, the computer-actionable TMV that is generated (e.g., TMV **400** of **Fig. 4**) is transmitted to a

plurality of target systems (e.g., target systems **540** of **Fig. 5**) for processing by the plurality of target systems.

II. Claim 9

Independent Claim 9 is directed to a system for generating computer security threat management information. An example of such a system is the CSIRT server **510** of **Fig. 5** of the present application. The system (e.g., server **510**) includes a Threat Management Vector (TMV) generator, such as message encoder **520** of **Fig. 5**, that is configured to generate a computer-actionable TMV (e.g., TMV **400** of **Fig. 4**) that is suitable for use by an automated threat management system such as, for example, the automated threat management systems that may be located at the Target Systems **540** illustrated in **Fig. 5** of the present application. The TMV generator (e.g., message encoder **520** of **Fig. 5**) generates the TMV (e.g., TMV **400** of **Fig. 4**) from a notification of a computer security threat that is received, for example, from one of the sources **110**, **120**, **130**, **160**, **170**, **180** or **190** of **Fig. 5**. The TMV (e.g., TMV **400** of **Fig. 4**) includes a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat (e.g., field **401** in **Fig. 4**), a second computer-readable field that provides identification of a release level for the system type (e.g., field **402** in **Fig. 4**) and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (e.g., field **403** in **Fig. 4**).

III. Claim 18

Independent Claim 18 is directed to a computer-actionable computer security Threat Management Vector (TMV) such as the TMV **400** of **Fig. 4**. The TMV includes (1) a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat (e.g., field **401** in **Fig. 4**), (2) a second computer-readable field that provides identification of a release level for the system type (e.g., field **402** in **Fig. 4**) and (3) a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (e.g., field **403** in **Fig. 4**). The TMV is in a format suitable for use by an automated threat management system such as, for example, the automated threat management systems that may be located at the Target Systems **540** illustrated in **Fig. 5**.

Grounds of Rejection to be Reviewed on Appeal

1. The rejections of Claims 1-23 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2003/0084349 to Friedrichs et al. ("Friedrichs").

Argument

I. The Rejections of Claims 1-23 as Anticipated by Friedrichs Should be Reversed

As noted above, Claims 1-23 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2003/0084349 to Friedrichs. Appellants respectfully submit for the reasons presented below that Friedrichs does not anticipate any of the pending claims. Section A below briefly discusses the "early warning" system of Friedrichs. Sections B-S then present Appellants' basis for contending that various sub-groups of Claims 1-23 are patentable over Friedrichs.

A. Introduction

Friedrichs is directed to an "early warning system for network attacks." (Friedrichs at Title). In the system/methods of Friedrichs, a plurality of security devices record information relating to security events that occur across a network. (*See, e.g.*, Friedrichs at ¶ 17). Some of this information is then extracted and written into a file having a common format. (*See, e.g.*, Friedrichs at ¶ 18). The information may then be transferred to a database server, where it may be converted into a common, vendor-independent format and analyzed. (*See, e.g.*, Friedrichs at ¶¶ 19 and 23-24). Finally, reports may be generated based on the analyzed data, and these reports are made available to users. (*See, e.g.*, Friedrichs at ¶ 25). The information provided to the user "may contain reports, graphs of security event data and other information related to the processing and analysis of security events and the detection of security incidents", user-requested "specific reports . . . on event data" and/or a "set of reports outlining recent abnormal activity." (Friedrichs at ¶ 26). The reports may be made available to users via a web server, e-mail, pager, facsimile or other delivery mechanisms. (*See, e.g.*, Friedrichs at ¶ 25).

Appellants respectfully submit that Friedrichs is simply another example of the labor-intensive prior art security threat management systems described in the background section of

the present application. Users of the system –i.e., individuals – of Friedrichs are provided written reports containing processed security event data. Each such user must then determine how to respond to the security threats contained within the reports and implement such responses. This is exactly the labor-intensive intervention process that embodiments of the present invention avoid. Thus, for the reasons discussed in more detail below, Appellants respectfully submit that Friedrichs does not anticipate any of the pending claims and, consequently, Appellants respectfully request reversal of the pending rejections.

B. The Rejection of Claims 1, 7 and 8

Claim 1 recites:

> 1. A method of generating computer security threat management information, comprising:
>
> receiving notification of a computer security threat;
>
> generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and
>
> transmitting the computer-actionable TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

Appellants submit that Friedrichs does not disclose at least four (4) of the recitations of Claim 1 and that, as such, the rejection of Claim 1 as anticipated by Freidrichs should be reversed. Claims 7 and 8 depend from Claim 1, and hence the rejections of Claims 7 and 8 should be reversed for at least the reasons that the rejection of Claim 1 should be reversed.

1. Friedrichs Does Not Disclose Generating a Computer Actionable TMV that is Transmitted to a Plurality of Target Systems

As an initial matter, Appellants submit that Friedrichs does not disclose "generating a **computer-actionable** Threat Management Vector (TMV) that is **suitable for use by an automated threat management system**" that is transmitted "to a plurality of target systems" as recited in Claim 1. Instead, the identified "TMV" of Friedrichs is a **report** that outlines security

event activity that led to the alert and may contain graphs that depict relevant security event data. (*See, e.g.*, Final Action at p. 8, citing to Friedrichs at ¶ 39). As discussed above, the information that is actually output or sent to users is "reports, graphs of security event data and other information related to the processing and analysis of security events and the detection of security incidents", user-requested "specific reports . . . on event data" and/or a "set of reports outlining recent abnormal activity." (Friedrichs at ¶ 26). These reports are made available to users via a web server, e-mail, pager, facsimile or other delivery mechanisms. (*See, e.g.*, Friedrichs at ¶ 25).

Appellants respectfully submit that Freidrich simply does not disclose or suggest generating and thereafter transmitting to a plurality of target systems a "computer-actionable" TMV that is "suitable for use by an automated threat management system" as recited in Claim 1. Instead, the information that is transmitted or otherwise made available to end users in Friedrichs are reports or graphs, neither of which are computer actionable. Thus, the system of Friedrichs does not disclose generating and then transmitting to target systems a **computer-actionable** Threat Management Vector (TMV) that is **suitable for use by an automated threat management system**" as recited in Claim 1.

In the Final Action, the Examiner further argues that paragraphs 8, 25 and 33 of Friedrichs demonstrate that Friedrichs generates a computer-actionable TMV. However, none of the cited portions of Friedrichs supports this assertion. In particular, paragraph [0008] from the "Summary" section of Freidrich describes how the system of Friedrichs uploads and then processes on a processor the security event information that the system has gathered. While this portion of Friedrichs discusses the computer processing of security event information, the processing that is described **is performed at the "early warning system"** of Friedrichs and is **not** processing that is carried out "at a plurality of target systems" that receive a TMV as recited in the last clause of Claim 1. (*See* Friedrichs at ¶¶ [0019] – [0024], describing the processing that is performed at the system of Freidrichs, and Friedrichs at ¶¶ [0025] – [0027], describing how **reports** containing security event data are then sent or displayed to the target users).

Paragraph [0025] of Friedrichs likewise does not support the pending rejection, but instead makes clear that the information that is actually transmitted to users is **not** "a computer-actionable . . . TMV that is suitable for use by an automated threat management system" as

recited in Claim 1. In fact, paragraph [0025] expressly states that the reports may be sent by **FAX or pagers** making clear that the reports are paper reports and not computer-actionable TMVs.

Paragraph [0033] similarly supports Appellants showing that Friedrichs does not disclose generating and transmitting to target systems a computer-actionable TMV. In particular, paragraph [0033] describes the first step (step **310**) of a method for processing security event data that is disclosed in the flow chart of Figure 3 of Friedrichs. This first step, like paragraph [0008] of Friedrichs, describes processing that is performed at the "early warning system" of Friedrichs as opposed to processing that is carried out at the "plurality of target systems." In fact, the flow chart of Figure 3 of Friedrichs (and the description thereof) expressly shows that information is sent to the users in the last step of the method (step **370**). Step **370** is described at paragraph [0039] of Freidrichs, and clearly indicates that the information that is sent to the users is not "computer actionable" information. (*See* Friedrichs at [0039] indicating, for example, that the "report may be delivered via a number of mechanism including email, cell phone, pager, SMS or fax").

2. Friedrichs Does Not Disclose the TMV Having First, Second and Third "Computer-Actionable" Fields of Claim 1

Appellants also respectfully submit that Friedrichs does not disclose a TMV having first, second and third "computer-readable fields" that contain the specific information specified in Claim 1. In computer science, a "field" is commonly known to refer to a separately-accessible sub-unit of data that has several parts. (*See, e.g.,* wikipedia.com, stating "In computer science, data that has several parts can be divided into fields. For example, a computer may represent today's date as three distinct fields: the day, the month and the year."). Appellants submit that there is no indication that the reports discussed in Friedrichs include the first, second and third fields of Claim 1, providing another basis for the reversal of the rejection of Claim 1.

In the Final Action, the Examiner argues that Friedrichs "discloses" the three specific pieces of information specified in Claim 1. (Final Action at p. 3). However, the Final Action does not even attempt to show that the "report" of Friedrich contains computer-readable fields that contain the specified information. Thus, the arguments in the Final Action fail to rebut

Appellants showing that Friedrichs does not disclose the TMV having first, second and third "computer-readable fields" of Claim 1.

3. Friedrichs Does Not Disclose a TMV Having a Field Identifying at Least One System that is Affected by the Security Threat

Appellants also submit that the cited portions of Friedrichs do not disclose a TMV having a field that provides "identification of at least one **system type that is affected by** the computer security threat." In particular, the Final Action cites to paragraphs 42 and 35 of Friedrich as disclosing this recitation of Claim 1 (Final Action at p. 9). However, what the cited portion of Friedrichs discloses is a Sensors database **405** that contains demographic information about the location, type and/or operating system of **the security devices that uploaded information** into the All-Events database or reported the security event. (Friedrichs at ¶ [0042]). Thus, the information relied on in the rejections relates to the security devices that report the security event, and clearly is not information identifying the "system type that is **affected by the computer security threat**" as recited in Claim 1. Appellants respectfully submit that the fact that a security device **reports** a security event does not mean that the reporting security device is **affected by** the computer security threat. Thus, the rejection of Claim 1 should also be reversed for this additional reason.

The Final Action cites to paragraph [0017] of Friedrichs as further support to the Examiner's contention that Friedrichs discloses a TMV having a field that provides identification of at least one **system type that is affected by** the computer security threat. (Final Action at p. 3). However, the cited portion of Friedrichs merely states that the security devices of Friedrichs may include anti-virus programs. This teaching of Friedrich does not indicate that Friedrichs discloses a TMV having a field that provides identification of at least one system type that is affected by the computer security threat.[1]

[1] The Final Action also argues, without explanation or support, that "it is only natural for the reporting system to send data pertinent to the affected system." (Final Action at p. 3). Appellants respectfully submit that such an unsupported and conclusory assertion is insufficient to support a rejection under 35 U.S.C. § 102.

4. Friedrichs Does Not Disclose a TMV Having a Field Identifying a Release Level for the System Type Affected

Appellants further submit that the cited portions of Friedrichs do not disclose a TMV having a field that provides "identification of a **release level** for the system type" **that is affected by** the computer security threat. In particular, the Final Action cites to paragraph 42 of Friedrich as disclosing this recitation of Claim 1 (Final Action at p. 9). However, the "type" information discussed in Friedrichs relates to the type of security device **that is uploading information** as opposed to the type of device that is **affected by** the security threat, and there is no indication that any "release" information is even provided. Thus, the rejection of Claim 1 should also be reversed for this additional reason.

In the Final Action, the Examiner further argues that release information would inherently be provided. (Final Action at p. 4). However, this argument fails for at least two reasons. First, there is no basis for the assertion that release information would be inherently – i.e., necessarily – provided. Second, as noted above, the information provided relates to the security device that is uploading information, and hence does not provide any information regarding the type of device that is **affected by** the security threat. Thus, the arguments in the Final Action fail to rebut Appellants showing.

C. The Rejection of Claim 2

Claim 2 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over Friedrichs. Claim 2 recites that the "generating" operation of Claim 1 involves "selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format." The Final Action cites to paragraphs 40-46 of Friedrichs as disclosing the recitations of Claim 2; however, the cited portions of Friedrichs make no mention of selecting system type, release and possible countermeasures from a database and then converting this information into a computer-readable format for inclusion in a TMV. Accordingly, Claim 2 is independently patentable over Friedrichs.

In the Final Action, the Examiner argues that the system type, release level and possible countermeasures are all stored in a database in Friedrichs. (Final Action at p. 5). Appellants respectfully submit that Friedrichs does not support this assertion. More importantly, the "database" of Friedrich is not a TMV that is transmitted to a plurality of target systems as recited in Claim 1. Accordingly, Claim 2 is independently patentable over Friedrichs.

D. The Rejection of Claim 3

Claim 3 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over Friedrichs. Claim 3 recites that the "system type comprises a computer operating system type" and that "the release level comprises a computer operating system release level." The Final Action cites to paragraphs 35 and 42 of Friedrichs as disclosing the recitations of Claim 3, and further argues that Friedrichs "inherently" discloses the recitation of Claim 3. (Final Action at p. 10 and 5). However, the cited portions of Friedrichs make no mention of the release level as recited in Claim 3 and, as discussed above with respect to the rejection of Claim 1, the Examiner has not and cannot show that this information would be "inherently" – i.e., necessarily -- provided. Accordingly, Claim 3 is also independently patentable over Friedrichs.

E. The Rejection of Claim 4

Claim 4 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over Friedrichs. Claim 4 recites that "the set of possible countermeasures comprises an identification of a countermeasure mode of installation." The Final Action cites to paragraph 45 of Friedrichs as disclosing the recitations of Claim 4. (Final Action at p. 10). However, paragraph 45 of Friedrichs discusses a separate Vulnerabilities database 440 and a Product database 450. The product database may include details on how to patch a particular flaw. However, there is no indication that the information in the Products database **is in a computer-actionable format**, and it is clear that the information in the Products database 450 is not part of the report (i.e., the alleged TMV) that is sent to the users. Accordingly, Claim 4 is also independently patentable over Friedrichs.

In the Final Action, the Examiner argues that Friedrichs provides data to a processor. (Final Action at 6). While this may be the case, what Claim 1 discusses is a computer actionable TMV that is transmitted to a plurality of target systems. The Final Action does not and cannot contend that the processor of Freidrich (or the information submitted thereto) is a "computer actionable TMV." It is also indisputable that Friedrich does not disclose or suggest transmitting such a "computer actionable TMV" to a plurality of target systems. Accordingly, the arguments in the Final Action fail to address or rebut Appellants showing with respect to the patentability of Claim 4.

F. The Rejection of Claim 5

Claim 5 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over Friedrichs. Claim 5 recites that "at least one of the identifications comprises a pointer." The Final Action states that "pointers are broadly used in databases to identify data," implicitly conceding that the recitation of Claim 5 is not disclosed in Friedrich. (Final Action at 10). The Final Action further argues that Friedrichs disclosure of a database "inherently" discloses a pointer. (Final Action at pp. 6-7). However, even, assuming, for the sake of argument, that pointers are broadly used in databases and hence "inherently" disclosed, the alleged TMV in Friedrichs (i.e., the information that is distributed) is not a database, but a report. As such, it is clear that Friedrichs also does not disclose or suggest the recitation added by Claim 5.

G. The Rejection of Claim 6

Claim 6 depends from Claim 1 and hence is patentable for at least the reasons, discussed above, that Claim 1 is patentable over Friedrichs. Claim 6 recites that the TMV further includes "a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level." The Final Action states that the description of the Security Device 110 and Hunter server 140 in paragraph [0022] of Friedrich discloses the recitations of Claim 6. (Final Action at 7 and

10-11). Notably, the Final Action does not even attempt to explain how these devices of Friedrichs correspond to the recitations of Claim 6, and Appellants respectfully submit that no such explanation could be provided. Accordingly, the Final Action likewise has failed to make a *prima facie* rejection with respect to the recitations added by Claim 6.

H. The Rejections of Claims 9, 16 and 17

Claims 9, 16 and 17 appear to stand rejected based on the same rationale as Claims 1, 7 and 8, respectively. Accordingly, Appellants respectfully submit that the rejections of Claims 9, 16 and 17 should be reversed for the same reasons, discussed above, that the rejections of Claims 1, 7 and 8, respectively, should be reversed.

I. The Rejection of Claim 10

Claim 10 appears to stand rejected based on the same rationale as Claim 1. Accordingly, Appellants respectfully submit that the rejection of Claim 10 should be reversed for the same reasons, discussed above, that the rejections of Claim 1 should be reversed.

J. The Rejection of Claim 11

Claim 11 appears to stand rejected based on the same rationale as Claim 2. Accordingly, Appellants respectfully submit that the rejection of Claim 11 should be reversed for the same reasons, discussed above, that the rejections of Claim 2 should be reversed.

K. The Rejection of Claim 12

Claim 12 appears to stand rejected based on the same rationale as Claim 3. Accordingly, Appellants respectfully submit that the rejection of Claim 12 should be reversed for the same reasons, discussed above, that the rejections of Claim 3 should be reversed.

L. The Rejection of Claim 13

Claim 13 appears to stand rejected based on the same rationale as Claim 4. Accordingly, Appellants respectfully submit that the rejection of Claim 13 should be reversed for the same reasons, discussed above, that the rejections of Claim 4 should be reversed.

M. The Rejection of Claim 14

Claim 14 appears to stand rejected based on the same rationale as Claim 5. Accordingly, Appellants respectfully submit that the rejection of Claim 14 should be reversed for the same reasons, discussed above, that the rejections of Claim 5 should be reversed.

N. The Rejection of Claim 15

Claim 15 appears to stand rejected based on the same rationale as Claim 6. Accordingly, Appellants respectfully submit that the rejection of Claim 15 should be reversed for the same reasons, discussed above, that the rejections of Claim 6 should be reversed.

O. The Rejections of Claims 18 and 23

Claims 18 and 23 appear to stand rejected based on the same rationale as Claims 1 and 8, respectively. Accordingly, Appellants respectfully submit that the rejection of Claims 18 and 23 should be reversed for the same reasons, discussed above, that the rejections of Claims 1 and 8, respectively, should be reversed.

P. The Rejection of Claim 19

Claim 19 appears to stand rejected based on the same rationale as Claim 3. Accordingly, Appellants respectfully submit that the rejection of Claim 19 should be reversed for the same reasons, discussed above, that the rejections of Claim 3 should be reversed.

Q. The Rejection of Claim 20

Claim 20 appears to stand rejected based on the same rationale as Claim 4. Accordingly, Appellants respectfully submit that the rejection of Claim 20 should be reversed for the same reasons, discussed above, that the rejections of Claim 4 should be reversed.

R. The Rejection of Claim 21

Claim 21 appears to stand rejected based on the same rationale as Claim 5. Accordingly, Appellants respectfully submit that the rejection of Claim 21 should be reversed for the same reasons, discussed above, that the rejections of Claim 5 should be reversed.

S. The Rejection of Claim 22

Claim 22 appears to stand rejected based on the same rationale as Claim 6. Accordingly, Appellants respectfully submit that the rejection of Claim 22 should be reversed for the same reasons, discussed above, that the rejections of Claim 6 should be reversed.

II. Conclusion

In light of the above, Appellants submit that each of the pending claims is patentable over the cited references and, therefore, request reversal of the rejections of Claims 1-23.

Respectfully submitted,

D. Randal Ayers
Registration No. 40,493

USPTO Customer No. 20792
Myers Bigel Sibley & Sajovec, P.A.
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

CERTIFICATION OF ELECTRONIC TRANSMISSION UNDER 37 CFR § 1.8

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent and Trademark Office on February 2, 2007.

Michele P. McMahan
Date of Signature: February 2, 2007

CLAIMS APPENDIX
Pending Claims USSN 10/624,344
Filed July 22, 2003

1. A method of generating computer security threat management information, comprising:

receiving notification of a computer security threat;

generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and

transmitting the computer-actionable TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

2. A method according to Claim 1 wherein the generating comprises selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format.

3. A method according to Claim 1 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

4. A method according to Claim 1 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

5. A method according to Claim 1 wherein at least one of the identifications comprises a pointer.

6. A method according to Claim 1 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level.

7. A method according to Claim 6 wherein the subsystem type comprises an application program type.

8. A method according to Claim 1 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

9. A system for generating computer security threat management information, comprising:

a Threat Management Vector (TMV) generator that is configured to generate a computer-actionable TMV that is suitable for use by an automated threat management system from a notification of a computer security threat that is received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level.

10. A system according to Claim 9 wherein the TMV generator is also configured to transmit the TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

11. A system according to Claim 9 further comprising a common semantics database that lists system types, release levels and possible countermeasures in a computer-readable format, wherein the TMV generator is responsive to the common semantics database to generate the TMV based upon user selection of a system type, release level and possible countermeasures from the common semantics database for the computer security threat.

12. A system according to Claim 9 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

13. A system according to Claim 9 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

14. A system according to Claim 13 wherein the set of possible countermeasures further comprises a pointer to a remediation to be applied as a countermeasure.

15. A system according to Claim 9 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level.

16. A system according to Claim 15 wherein the subsystem type comprises an application program type.

17. A system according to Claim 9 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

18. A computer-actionable computer security Threat Management Vector (TMV) comprising:

a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat;

a second computer-readable field that provides identification of a release level for the system type; and

a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level,

wherein the TMV is in a format suitable for use by an automated threat management system.

19. A TMV according to Claim 18 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

20. A TMV according to Claim 18 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

21. A TMV according to Claim 18 wherein at least one of the identifications comprises a pointer.

22. A TMV according to Claim 18 further comprising:

a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat;

a fifth computer-readable field that provides identification of a release level for the subsystem types; and

wherein the third computer-readable field provides identification of a set of possible countermeasures for a subsystem type and a release level.

23. A TMV according to Claim 18 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

EVIDENCE APPENDIX

No evidence is being submitted with this *Appeal Brief* pursuant to 37 C.F.R. §§ 1.130, 1.131 or 1.132.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.